відносяться сигнатурні засоби, зокрема, системи IDS/IPS, побудовані за сигнатурним принципом. Прискорити ресурсоємну процедуру множинного розпізнавання патернів в таких системах дозволяють апаратні пристрої на базі ПЛІС.

Метою даної роботи є дослідження можливостей та особливостей використання пристроїв програмованої логіки в якості апаратної платформи для побудови сигнатурних систем технічного захисту інформації в кіберфізичних системах енергетичної галузі.

В результаті аналізу існуючих кіберфізичних систем, знайдено два класи технічних засобів, що містять ПЛІС, на яких можуть бути реалізовані апаратні засоби захисту інформації. По-перше, це системи управління, що використовують такі інтелектуальні технології як нейронні мережі та нечітку логіку, інтелектуальні системи збору даних, частотні перетворювачі для електроприводів тощо. По-друге, деякі "розумні" електронні пристрої (Intelligent Electronic Devices – IED) , які також використовуються технологією Smart Grid кіберфізичних систем містять ПЛІС і системи на кристалі. Реконфігурація (оновлення обчислювальної структури) програмованих пристроїв може бути виконано віддалено. Проте даний процес необхідно захистити, оскільки канал зв'язку привносить потенційну вразливість у разі фізичного доступу зловмисника до мережі. В роботі розглянуто безпечний протокол і реконфігуровний модуль на ПЛІС, який використовується для налаштування та моніторингу мережевих IP-адрес. Запропонована полегшена версія протоколу другого рівня, реалізованого повністю апаратно та захищеного криптографічним алгоритмом AES-GCM відповідно до стандарту IEC 61850-90-5.

Висновки. ПЛІС, що задіяні в пристроях промислової автоматики, а також входять до складу інтелектуального цифрового обладнання, можуть бути використані для синтезу в них апаратних систем захисту інформації. Для безпечної віддаленої конфігурації ПЛІС, що використовуються в засобах захисту кіберфізичних систем, необхідно вживати додаткові заходи.

УДК 004.681.3

АЛГОРИТМ СТРУКТУРНОЇ ІДЕНТИФІКАЦІЇ ПРОГНОЗУЮЧИХ МОДЕЛЕЙ

[1]Хорошко Володимир Олексійович, [2]Хохлачова Юлія Євгенівна, [3]Вишневська Наталія Сергіївна

Національний авіаційний університет

[1]professor@ukr.net,

[2]yuliiahohlachova@gmail.com, [3]nataliia.vyshnevska@npp.nau.edu.ua

Прогнозування кіберзахищеності об'єктів є одним із вирішальних наукових факторів формування стратегії та тактики кіберзахисту.

Для прогнозування та моделювання процесів кіберзахисту найбільш прийнятними є статистичні методи, що ґрунтуються на існуючих тенденціях у змінах показників кіберзахищеності.

Моделі прогнозування можуть бути як довгостроковими, так і короткостроковими. Внаслідок широкого ступеня невизначеності в отриманні інформації пріоритетне значення надається короткостроковим прогнозам.

Невід'ємною складовою завдань управління (оптимального, автоматизованого чи на рівні прийняття рішень) є побудова моделей, які описують чи прогнозують поведінку об'єкта, процесу системи. У випадку отримання математичної моделі необхідно вибрати її структуру і оцінити параметри, тобто розв'язати задачу структурної ідентифікації.

Структурна ідентифікація сприймається, як завдання перешкоди структури моделі з мінімальною дисперсією помилки прогнозування.

Існують різноманітні постановки завдання структурної ідентифікації, методи її вирішення та варіанти програмної реалізації, розроблені фахівцями у галузях ідентифікації, прикладного регресійного аналізу та пошуку залежностей.

Більшість методів побудовано різних підходах, що ускладнює порівняльний аналіз визначення умов їх ефективного застосування. Оскільки для завдань управління важливо будувати моделі з меншою помилкою прогнозування, це є основою для порівняння ефективності існуючих підходів.

Найбільш поширеними є дві групи методів, на основі яких будують моделі для прогнозування: описання взаємодії процесів кіберзахисту різного рівня на основі вивчення внутрішніх механізмів функціонування процесів, що моделюються, та представлення отриманих знань; отримання моделей за допомогою оцінювання параметрів за вибірками спостережень із застосуванням регресійного аналізу.

У загальному випадку процес вирішення задачі структурно-параметричної ідентифікації включає наступні основні етапи: завдання вибірки даних до апріорної інформації; вибір чи завдання класу базисних функцій та перетворення даних; генерація різних структур у вибраному класі; оцінювання параметрів генерованих структур та формування безлічі моделей F; мінімізація заданого критерію та вибір оптимальної моделі f; перевірка адекватності отриманої оптимальної моделі; ухвалення рішення про завершення процесу.

Перелічені етапи описують довільний процес побудови моделей, причому залежно від апріорної інформації та мети моделювання ті чи інші етапи можуть бути відсутніми.

Для складних об'єктів кіберзахисту та процесів типовою є невизначеність інформації щодо механізму їх функціонування, ступеня інформативності вимірювальних змінних та властивостей. При цьому необхідно застосовувати формалізовані методи та автоматизовані способи моделювання.

Тому актуальною є проблема розробки алгоритму структурної ідентифікації прогнозуючих моделей з метою створення автоматизованих способів оптимального вибору структури моделей складних об'єктів за вибірками обмеженого обсягу в умовах неповної інформації.

Алгоритм складається з наступних кроків:

Крок 1. Вказується початкова матриця приватних описів Z^0 (для неї вважають $s = 0$):

$$Z^0 = \left[O \vdots o \vdots I \vdots X\right] = \left[O \vdots \overline{C}^0\right], \quad (1)$$

де o – нульовий вектор (розмірності N);
O – нульова матриця (розмірності $N \times F$);
I – одиничний вектор (розмірності N);
$X = \left[x_1 \vdots x_2 \vdots x_3 \vdots ... x_m \vdots\right]$ – матриця спостережень вхідних змінних (розмірності $N \times F$).

Крок 2. Визначається вектор R.

Нехай вектори $\overline{z}^r$ будуються за правилом:

$$\overline{z}^r(i) = \overline{a} \cdot \overline{z}^r_{j1}(i) + \overline{b}\overline{z}^{r-1}_{j2}(i) \cdot \overline{Z}^{r-1}_{j3}(i), \quad (2)$$

де $z = 1, 2, 3, ...$ – номер ітерації;
$i = 1, 2, 3, ..., N$ – номер спостереження, який для зручності запису взято у дужки;
$j_1, j_2, j_3 = 1, 2, 3, ..., F + 2 + m + 2s, (j_3 \geq j_2)$ – номери приватних описів із матриці $\overline{Z}^{r-1}$;
$\overline{a}, \overline{b}$ - коефіцієнти, що визначаються на навчальній підвиборці спостережень (A).

Значення коефіцієнтів ($\overline{a}$) і ($\overline{b}$) перебувають як розв'язання задачі мінімізації:

$$\overline{a}, \overline{b} = \arg\min_{a,b} \Phi(a,b), \quad \Phi(a,b) = \sum_{i=1}^{N(A)} e_A^2(i), \quad (3)$$

де $e_A(i)$, $i = 1, 2, ..., N(A)$ – залишки в регресії y_A за двома змінними

$$y_A(i) = a \cdot \overline{Z}^{r-1}_{j_1}(i) + b \cdot \overline{Z}^{r-1}_{j_2}(i) \cdot \overline{Z}^{r-1}_{j_3 A}(i) + e_A(i). \quad (4)$$

З усіх генерованих за правилом (9)-(11) приватних описів відбираються F описів кращих мінімуму квадратичної норми залишків на перевірочній підвиборці спостережень B:

$$J = \frac{1}{N(B)} \sum_{i=1}^{N(B)} \bar{e}_B(i),$$
$$\bar{e}_B(i) = y_B(i) - \bar{Z}^r_B,$$
$$\bar{Z}^r_B = \bar{a} \cdot \bar{Z}^{r-1}_{j_1 B}(i) + b \cdot \bar{Z}^{r-1}_{j_2 B}(i) \cdot \bar{Z}^{r-1}_{j_3 B}(i), \quad (5)$$

де $N(B)$ – обсяг перевірочної добірки B.

Відібрані найкращі приватні описи, ранжирувані за зменшенням величини J, використовуються при формуванні матриці

$$\bar{G}^r = \left[\bar{z}^r_1 : \bar{z}^r_2 : \ldots \bar{z}^r_F : \right]. \quad (6)$$

Матриця $\bar{C}^r$ не змінюється $\bar{C}^r = \bar{C}^{r-1}$.

Матриця $\bar{D}^r$ формується з урахуванням структури кращого із F відібраних приватних описів ($\bar{Z}^r_F$). Перші S стовпці матриці $\bar{D}^r$ заповнюються окремими елементами кращого приватного опису за правилом:

$$\bar{d}^r_h(i) = \bar{Z}^r_{F+2+m+2s}(i) = \theta_h \prod_{j=1}^{m} x_j^{\alpha_{h_j}}(i) \quad (7)$$

де $h = 1, 2, 3, \ldots, s$ – номер члена у структурі;

s - число членів у структурі кращого приватного опису;

Другі s стовпців матриці $\bar{D}^r$ формуються почерговим винятком окремих членів із структури приватного опису за правилом

$$\bar{d}^r_{s+h}(i) = \bar{Z}^r_{F+2+m+s+h}(i) = \sum_{\substack{q=1 \\ (q \neq h)}}^{s} \bar{\theta}_q \prod_{j}^{m} x_j^{d_{jq}}(i) \quad (8)$$

Таким чином визначається оператор R перетворення

$\bar{Z}^{r-1} \xrightarrow{R} Z^r$.

Правило обстановки для ітераційної схеми: обчислення закінчуються на ітерації r^*, якщо виконується умова

$$J(\bar{Z}^{r^*-1}_F) - J(\bar{Z}^{r^*}_F) < \delta_z \quad (9)$$

де $J(\overline{Z}_F^{r^*})$ – значення критерію для найкращого приватного опису ітерації r;

δ_z – задане число.

Особливістю алгоритму є багатоповерховість. Номер поточного етапу визначає максимально можливу кількість членів у моделях. Синтез моделей починається з етапу з номером $p=1$ чи з будь-якого заданого номера p^0. Кожен етап є ітераційною схемою (8)-(16). Початкова матриця приватних описів етапу з номером p задається кінцевою матрицею приватних описів попереднього етапу

$$\overline{Z}_p^0 = \overline{Z}_{p-1}^{r^*} \tag{10}$$

а для $p = p^0$ вона збігається з (8). Обчислення закінчується на етапі p^*, якщо виконано умову

$$J(\overline{Z}_{F_1 p^*-1}^{r^*}) - J(\overline{Z}_{F_1 p^*}^{r^*}) < \delta_p, \tag{11}$$

де $J(\overline{Z}_{F_1 p^*}^{r^*})$ – значення критерію для кращого частного опису r-й ітерації етапу p;

δ_p – задане число.

Відмінні риси алгоритму: багатоповерховість моделі; пошук моделі, як у класі лінійних, так і в класі нелінійних за вхідними змінними моделями; прийоми виключення окремих членів кращого приватного опису та на основі цього розширення базисного набору аргументів; оптимальність за обчислювальними витратами для ітераційних алгоритмів методу групового обліку аргументу (МГОА) схеми розрахунку критерію іспиту, що ковзає; можливість оцінювати коефіцієнти у моделях як за методом найменших квадратів, так і за методом найменших модулів.